

คุณลักษณะด้านเทคนิคขั้นต่ำและขอบเขตการดำเนินงาน
การจ้างผู้ให้บริการสิทธิการใช้งานและบำรุงรักษาระบบ File Integrity Monitoring (FIM)

ผู้ยื่นข้อเสนอต้องเสนอบริการ โดยมีคุณลักษณะด้านเทคนิคขั้นต่ำอย่างน้อยดังนี้

1. ข้อกำหนดความต้องการทั่วไป

ผู้ยื่นข้อเสนอต้องเสนอบริการระบบ (FIM) ที่สามารถทำงานได้ตามวัตถุประสงค์ของ ธสน. และสามารถทำงานร่วมกับระบบคอมพิวเตอร์และระบบเครือข่ายของธนาคารที่ใช้งานอยู่ในปัจจุบันตลอดจนสามารถรองรับการขยายงานในอนาคตของธนาคาร ได้อย่างมีประสิทธิภาพ

- 1.1. สามารถบริหารจัดการอุปกรณ์ผ่าน Web Browser หรือ Software Agent ได้
- 1.2. ผู้ยื่นข้อเสนอต้องเสนอสิทธิการใช้งานระบบฐานข้อมูล Microsoft SQL Server Standard 2019 และจำนวน Cals License ให้ครอบคลุมกับการใช้งานกับระบบที่นำเสนอ
- 1.3. กรณีที่มีได้มีการกำหนดคุณสมบัติเฉพาะไว้หากจำเป็นต้องเพิ่มเติมเพื่อให้บริการระบบ (FIM) สามารถทำงานได้อย่างถูกต้อง ครบถ้วน และสมบูรณ์ ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกต้องจัดหา Hardware หรือ Software หรือ License หรือส่วนประกอบเพิ่มเติมที่จำเป็นต่อการปรับปรุง และติดตั้ง ระบบ File Integrity Monitoring (FIM) ของธนาคารในครั้งนี้ให้ครบถ้วนโดยไม่มีค่าใช้จ่ายเพิ่มเติม

2. ข้อกำหนดคุณสมบัติเฉพาะของบริการระบบ (FIM)

- 2.1 เป็นโซลูชันบริหารจัดการกำหนดค่าความปลอดภัย (Security Configuration Management) โดยมีความสามารถในการตรวจสอบความถูกต้องของระบบ (Integrity Monitoring) และการตั้งค่าตาม Compliance (Configuration and Compliance Management) ได้
- 2.2 ระบบที่นำเสนอจะต้องเป็นแบบ Software-based
- 2.3 ระบบที่นำเสนอรองรับการตรวจสอบข้อมูล File Systems บนระบบปฏิบัติการ (OS) อย่างน้อย 4 ระบบ อุปกรณ์ ได้แก่ Windows, Red Hat, CentOS, Ubuntu, SUSE, AIX และ Solaris โดยจะต้องมีสิทธิการใช้งานถูกต้องตามกฎหมาย (License) อย่างน้อย 4 Licenses หากระบบที่นำเสนอไม่สามารถทำได้ ทางผู้ยื่นข้อเสนอสามารถนำระบบอื่นเพิ่มเติม เพื่อให้มีความสามารถตามข้อกำหนดได้
- 2.4 ระบบที่นำเสนอรองรับการตรวจสอบข้อมูล Database เช่น Oracle, MS SQL, DB2 โดยจะต้องมีสิทธิการใช้งานถูกต้องตามกฎหมาย (License) อย่างน้อย 1 License
- 2.5 ระบบที่นำเสนอต้องรองรับการตรวจสอบข้อมูลของ Network Device โดยจะต้องมีสิทธิการใช้งานถูกต้องตามกฎหมาย (License) อย่างน้อย 3 Licenses
- 2.6 ระบบที่นำเสนอต้องทำงานได้ทั้งแบบ Agent และ Agentless
- 2.7 ระบบที่นำเสนอจะต้องสามารถแสดงผลการตรวจสอบตาม Compliance หรือ Framework ได้อย่างน้อย ดังนี้
 - SWIFT
 - ISO
 - PCI
 - NIST
 - MITRE
 - CNSSI
- 2.8 ระบบที่นำเสนอต้องมีความสามารถในการกำหนดค่า Compliance แบบ customized compliance ได้
- 2.9 ระบบที่นำเสนอต้องสามารถใช้ compliance ที่แตกต่างกันตรวจสอบระบบงานเดียวกันได้
- 2.10 ระบบที่นำเสนอจะต้องแสดงรายละเอียดของการ Compliance รวมถึงแสดงข้อมูลวิธีแก้ไขพบเมื่อสิ่งที่ไม่สอดคล้องกับข้อกำหนดเพื่อให้ผ่าน Compliance หรือ Framework ตามข้อ 2.7 ได้

- 2.11 ระบบที่นำต้องสามารถทำการตรวจสอบ Compliance ได้ด้วยตนเอง หรือตาม Schedule ได้
- 2.12 ระบบที่นำเสนอต้องสามารถแสดงข้อมูลการทำ Compliance ย้อนหลังได้ 6 เดือนเป็นอย่างน้อยเพื่อทำการเปรียบเทียบผลการดำเนินงาน
- 2.13 ระบบที่นำเสนอจะต้องแสดงข้อมูลเมื่อมีการเปลี่ยนแปลงค่า Configuration ในระบบได้ดังนี้
- แสดงข้อมูลจริงก่อนและหลังที่เปลี่ยนแปลงไปจากเดิม
 - แสดงข้อมูล hash ของไฟล์ก่อนและหลังที่เปลี่ยนแปลงไปจากเดิม
 - แสดงชื่อผู้ใช้งานที่ดำเนินการ
 - แสดงเวลาทำการแก้ไขข้อมูล
- หากระบบที่นำเสนอไม่สามารถทำได้ ทางผู้ยื่นข้อเสนอสามารถนำระบบอื่นเพิ่มเติม เพื่อให้มีความสามารถตามข้อกำหนดได้ โดยไม่มีค่าใช้จ่ายเพิ่มเติมต่อธนาคาร
- 2.14 ระบบ FIM ที่นำที่เสนอจะต้องสามารถกำหนดค่าแรกเริ่มของข้อมูล โดยต้องสามารถเปลี่ยนแปลงค่าแรกเริ่มของข้อมูลตามความเหมาะสมของธนาคาร หากระบบที่นำเสนอไม่สามารถทำได้ ผู้ยื่นข้อเสนอสามารถนำระบบอื่นเพิ่มเติม เพื่อให้มีความสามารถตามข้อกำหนดได้
- 2.15 ระบบที่นำเสนอที่เสนอรองรับกำหนดค่าการตั้งเวลา หรือการตรวจสอบการเปลี่ยนแปลงของไฟล์แบบ Real-time ของ File Systems และ Databases หากระบบที่นำเสนอไม่สามารถทำได้ ผู้ยื่นข้อเสนอสามารถนำระบบอื่นเพิ่มเติม เพื่อให้มีความสามารถตามข้อกำหนดได้
- 2.16 ระบบที่นำเสนอจะต้องทำการเก็บ Log การเปลี่ยนแปลงของไฟล์ เช่น เพิ่ม ลบ และเปลี่ยนแปลง ไว้ภายในระบบได้ และสามารถส่งข้อมูล (Log) ไปยังระบบวิเคราะห์ข้อมูล (SIEM) ได้โดยใช้ Syslog Protocol
- 2.17 ระบบที่นำเสนอต้องสามารถแจ้งเตือนผ่านทาง Email ได้เมื่อมีการเปลี่ยนแปลงข้อมูลตาม Policy ที่กำหนดไว้
- 2.18 ระบบที่นำเสนอจะต้องรองรับติดตั้ง Agent บนระบบปฏิบัติการ Windows, Red Hat, CentOS, Ubuntu, SUSE
- 2.19 ระบบที่นำเสนอต้องสามารถตรวจสอบข้อมูลของ Network Device ได้ผ่าน SSH หรือ Telnet หากระบบที่นำเสนอไม่สามารถทำได้ ทางผู้ยื่นข้อเสนอสามารถนำระบบอื่นเพิ่มเติม เพื่อให้มีความสามารถตามข้อกำหนดได้
- 2.20 ระบบที่นำเสนอต้องมี REST API เพื่อสามารถทำงานร่วมกับซอฟต์แวร์ Third-party อื่นๆได้
- 2.21 ระบบที่นำเสนอสามารถสร้าง Local user หรือ สามารถทำการ Authentication ด้วย LDAP ได้ และต้องสามารถกำหนดสิทธิ์เฉพาะของ Admin ได้
- 2.22 ระบบที่นำเสนอต้องปรับแต่งค่า User-interface ตาม Role-based หรือสามารถ Customized ได้ เช่น Dashboards, Asset, Rules , Policy
- 2.23 ระบบที่นำเสนอสามารถจัดทำรายงาน หรือ Dashboard สรุปผลตาม compliance หรือ change ที่เกิดขึ้นบนระบบที่มีการ monitor ได้
- 2.24 ระบบที่นำเสนอสามารถปรับแต่งข้อมูลรายงาน (Custom Report) ได้ หากระบบที่นำเสนอไม่สามารถทำได้ ผู้ยื่นข้อเสนอสามารถนำระบบอื่นเพิ่มเติม เพื่อให้มีความสามารถตามข้อกำหนดได้
- 2.25 ระบบที่นำเสนอสามารถ export รายงานในรูปแบบ CSV, XML, HTML หรือ PDF ได้
- 2.26 ระบบที่นำเสนอต้องรองรับการ export และ import ค่า Setting ของระบบได้

3. ขอบเขตการดำเนินงาน

ผู้ยื่นข้อเสนอราคาที่ได้รับคัดเลือก ต้องดำเนินการตามขอบเขตที่กำหนดอย่างน้อยดังนี้

- 3.1 ต้องการติดตั้งบริการระบบ FIM รวมถึง Software บนอุปกรณ์ Server และ อุปกรณ์เครือข่ายให้กับธนาคาร ณ ที่ทำการสำนักงานใหญ่
- 3.2 ต้องดำเนินการติดตั้ง และทำการ Configuration และทดสอบตามเกณฑ์ที่ธนาคารกำหนด และต้องแก้ไขปัญหาจนกระทั่งสามารถใช้งานตามวัตถุประสงค์ของธนาคารโดยไม่มีค่าใช้จ่ายเพิ่มเติม

- 3.3 ต้องดำเนินการทดสอบความสามารถของระบบ File Integrity Monitoring (FIM) ในการตรวจจับเมื่อมีการเปลี่ยนแปลงไฟล์หรือค่าการติดตั้งของระบบธนาคารจากที่กำหนดไว้ พร้อมทั้งสามารถแจ้งเตือนเมื่อมีการเปลี่ยนแปลงหรือแก้ไขข้อมูล
- 3.4 ต้องจัดให้มีบุคลากรที่จะให้การสนับสนุนธนาคารระหว่างดำเนินการติดตั้งระบบ จนเสร็จตามระยะเวลาที่กำหนด
- 3.5 ต้องจัดทำเอกสารการใช้งานสำหรับผู้ใช้งาน ผู้ดูแลระบบที่ประกอบด้วยขั้นตอนการดูแลระบบและขั้นตอนในการค่าการตรวจสอบข้อมูล รวมถึงเอกสารคู่มือการทำงานของระบบอย่างละเอียด ซึ่งเอกสารที่ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกจัดทำขึ้นและส่งมอบให้แก่ธนาคารให้ตกเป็นกรรมสิทธิ์ของธนาคาร โดยมีรายละเอียดของเอกสารที่ต้องจัดทำดังนี้
 - 3.5.1 คู่มือการใช้งานระบบสำหรับผู้ใช้งานระบบ (User Manual)
 - 3.5.2 คู่มือการใช้งานระบบสำหรับผู้ดูแลระบบ (Operation Manual Administrator)
 - 3.5.3 คู่มือการทำงานของระบบ (System Detail & Diagram)
 - 3.5.4

4. ด้านการฝึกอบรม

- 4.1 ผู้ยื่นข้อเสนอต้องจัดฝึกอบรมเกี่ยวกับการใช้งานและการดูแลระบบ FIM พร้อมจัดทำเอกสารการฝึกอบรมให้แก่เจ้าหน้าที่ธนาคาร โดยการอบรมในห้องอบรมหรืออบรมผ่านช่องทางออนไลน์ที่ธนาคารมีรายละเอียดดังนี้
 - 4.1.1 หลักสูตรอบรมสำหรับผู้ใช้งานระบบ จำนวน 1 รอบ รอบละไม่น้อยกว่า 2 คน
 - 4.1.2 หลักสูตรสำหรับผู้ดูแลระบบ จำนวน 1 รอบ รอบละไม่น้อยกว่า 2 คน

5. การให้บริการสนับสนุนของบริการตลอดระยะเวลาการให้บริการ (Support)

ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือก จะต้องจัดให้มีบริการอย่างน้อยดังต่อไปนี้

- 5.1 ต้องจัดให้มีเจ้าหน้าที่ประสานงานที่มีความรู้ความเชี่ยวชาญ พร้อมหมายเลขโทรศัพท์ที่สามารถติดต่อได้สะดวกเพื่อรับแจ้งเหตุขัดข้อง ให้คำปรึกษา ตอบข้อซักถาม ให้ความช่วยเหลือหรือแก้ไขปัญหาเบื้องต้น (On Phone Support) รวมถึงช่องทางอื่นที่ธนาคารสามารถติดต่อขอรับคำปรึกษาได้ ในวันจันทร์ถึงวันศุกร์ ยกเว้นวันหยุดนักขัตฤกษ์ ตั้งแต่เวลา 8:30 น. – 18:00 น.
- 5.2 กรณีที่การใช้ระบบเกิดเหตุขัดข้องหรือชำรุดบกพร่อง และไม่สามารถแก้ไขปัญหาผ่านทางโทรศัพท์ และ/หรือช่องทางอื่นได้ ผู้ให้บริการต้องเข้ามาให้บริการตรวจสอบ แก้ไขปัญหา ณ สถานที่ติดตั้ง (Onsite Service) ได้ตลอด 24 ชั่วโมง (24x7) โดยมีรายละเอียดดังนี้
 - 5.2.1 กรณีปัญหาเร่งด่วนที่ทำให้ไม่สามารถใช้งานระบบได้: ต้องดำเนินการแก้ไขเหตุขัดข้องให้แล้วเสร็จภายใน 24 ชั่วโมง นับจากได้รับแจ้งเหตุเป็นอีเมลหรือโทรศัพท์
 - 5.2.2 กรณีระบบทำงานผิดพลาด ซึ่งเป็นส่วนสำคัญที่กระทบต่อการดำเนินงานของธนาคาร: ต้องดำเนินการแก้ไขเหตุขัดข้องให้แล้วเสร็จ ภายใน 48 ชั่วโมงนับจากได้รับแจ้งเหตุเป็นอีเมลหรือโทรศัพท์
 - 5.2.3 กรณีระบบทำงานผิดพลาด แต่ไม่ได้เป็นส่วนสำคัญที่กระทบต่อการดำเนินงานของธนาคาร: ต้องดำเนินการแก้ไขเหตุขัดข้องให้แล้วเสร็จ ภายใน 72 ชั่วโมงนับจากได้รับแจ้งเหตุเป็นอีเมลหรือโทรศัพท์
- 5.3 ต้องนำส่งรายละเอียดและขั้นตอนการแก้ไขปัญหา เหตุขัดข้อง และ/หรือความชำรุดบกพร่องของการใช้งานระบบ อย่างละเอียดให้แก่ธนาคารทันทีที่สามารถดำเนินการได้ และผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกตกลงเป็นผู้รับผิดชอบชำระค่าใช้จ่ายที่เกิดขึ้นจากการเข้าดำเนินการทั้งจำนวน
- 5.4 ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกต้องเข้าดำเนินการทำ Preventive Maintenance ทุก 3 เดือน โดยตรวจสอบดูแลระบบที่เสนอ ให้อยู่ในสภาพใช้งานได้ดีอยู่เสมอตลอดระยะเวลาการให้บริการ และต้องส่งมอบรายงานการให้บริการให้กับธนาคารภายใน 30 วัน หลังจากเข้าดำเนินการเสร็จสิ้นในแต่ละครั้ง